UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/628,315	07/28/2000	Kazuo Ezawa	AP32610-072817.0152	3474

21003 7590 02/03/2004

BAKER & BOTTS
30 ROCKEFELLER PLAZA
NEW YORK, NY 10112

EXAMINER	
VAUGHAN, MICHAEL R	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 02/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/628,315	EZAWA ET AL.	
	Examiner	Art Unit	
	Michael R Vaughan	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 June 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 June 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *3*.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-58 have been examined and are pending.

Information Disclosure Statement

2. An initialed and dated copy of Applicant's IDS form 1449, Paper No. 3 is attached to the instant Office action.

Claim Rejections - 35 USC ' 112, second paragraph

3. Claim 17 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The specification does not reinforce the meaning of "on-chip risk". The specification discloses –on-chip risk management. For purposes of this office action the examiner is interpreting "on-chip risk" and on-chip risk management. Clarification and/or correction are required.

Claim Rejections - 35 USC ' 112, first paragraph

4. Claims 17 is rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The specification does not reinforce the meaning of "on-chip risk". The specification discloses –on-chip risk management--. For purposes of this office action the examiner is interpreting "on-chip risk" and on-chip risk management.

Claim Rejections - 35 USC ' 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless --

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-3, 4-44, and 46-58 are rejected under 35 U.S.C. 102(b) as being anticipated by Claus (USP 5,461,217).

As per claim 1, Claus teaches a method for communicating between a first portable device having a first storage device and a second portable device having a second storage device, the first storage device storing thereon a first sequence number and a first key, the second storage device storing thereon a second sequence number and a second key, the method comprising the steps of (column 5, lines 53-53): comparing the first sequence number to the second sequence number (column 12, line 41); if the second sequence number is newer than the first sequence number, performing a verification using the first and second keys (column 12, lines 42-54); and setting the first sequence number to have a value of the second sequence number if the verification succeeds (column 12, line 55).

As per claims 25, Claus teaches a storage device storing a first sequence number and a first key (column 3, lines 20-25, column 8, line 10, and column 12, line 41)); and a processing device performing the following: receives a second sequence number and a second key from the further portable device (column 12, line 36), compares the first sequence number to the second sequence number (column 12, line 40-42),

if the second sequence number is newer than the first sequence number, performs a verification using the first and second keys (column 12, lines 42-54), and

sets the first sequence number to have a value of the second sequence number if the verification succeeds (column 12, line 55).

As per claim 32, Claus teaches the first portable device having a first storage device, the second portable device having a second storage device, the first storage device storing thereon a first sequence number, the second storage device storing thereon a second sequence number (column 5, lines 52-53), the method comprising the steps of: comparing the first sequence number to the second sequence number, the first sequence number being indicative of a first time provided on the first portable device, the second sequence number being indicative of a second time provided on the second portable device (column 12, line 41); and if the first time is older than the second time, setting the first sequence number to have a value of the second sequence number (column 12, lines 42-54).

As per claims 37, Claus teaches a storage device storing a first sequence number (column 5, lines 52-53); and a processing device performing the following: receives a second sequence number from the further portable device, compares the first sequence number to the second sequence number, the first sequence number being indicative of a first time provided on the portable device, the second sequence number being indicative of a second time provided on the further portable device (column 12, line 41), and

executes one of the following actions: if the first time is older than the second time, sets the first sequence number to have a value of the second sequence number (column 12, lines 42-54), and if the second time is older than the first time, sets the second sequence number to have a value of the first sequence number (column 7, lines 63-65).

As per claim 41, Claus teaches the first portable device having a first storage device, the second portable device having a second storage device, the first storage device storing thereon a first sequence number and a first key, the second storage device storing thereon a second sequence number and a second key (column 5, lines 52-53), the method comprising the steps of: comparing the first sequence number to the second sequence number, the first sequence number being indicative of a first time provided on the first portable device, the second sequence number being indicative of a second time provided on the second portable device (column 12, line 41); if the second time is newer than the first time, performing a verification using at least one of the first and second keys (column 12, lines 42-54); and setting the first sequence number to have a value of the second sequence number if the verification succeeds (column 12, line 55).

As per claim 54, Claus teaches a storage device storing a first sequence number and a first key (column 5, lines 53-53): and a processing device performing the following: receives a second sequence number and a second key from the further portable device (column 12, line 36), compares the first sequence number to the second

sequence number, the first sequence number being indicative of a first time provided on the portable device, the second sequence number being indicative of a second time provided on the further portable device (column 12, line 41), if the second time is newer than the first time, performs a verification using the first and second keys (column 12, lines 42-54), and sets the first sequence number to have a value of the second sequence number if the verification succeeds (column 12, line 55).

As per claims 2, 31, and 58, Claus teaches wherein the first key is a first global signing key, and the second key is a second global signing key, and wherein the verification is performed by comparing at least one first portion of the first global signing key to at least one second portion of the second global signing key (column 11, lines 13-16).

As per claim 3, Claus teaches wherein the verification succeeds when the at least one first portion corresponds to the at least one second portion (column 12, line 44).

As per claim 5, Claus teaches after the setting step, performing a transaction between the first card and the second card (column 12, lines 55-56).

As per claim 6, Claus teaches if the verification fails, suspending a transaction between the first card and the second card (column 11, line 18).

As per claims 7, 26, 48, and 55, Claus teaches if the verification fails, recording a failure of the verification in at least one of the first storage device and the second storage device (column 11, line 19).

As per claims 8, 27, and 58, Claus teaches if the first sequence number and the second sequence number are equal, performing a transaction between the first card and the second card (column 7, line 55—column 8, line 19).

As per claims 9 and 50, Claus teaches wherein the setting step is performed by transmitting an authenticated system message ("ASM") command from the second card to the first card, and wherein at least one of the first and second cards sets the second sequence number (column 12, line 50).

As per claims 10 and 28, Claus teaches the first storage device stores a third sequence number thereon, wherein the second storage device stores a fourth sequence number thereon (column 8, lines 9-26), and further comprising the steps of:

if the first sequence number and the second sequence number are equal, determining whether the third sequence number corresponds to the fourth sequence number (column 8, lines 20-27); and if the third sequence number does not correspond

to the fourth sequence number, transmitting an authenticated system message ("ASM") command from a particular card of the first and second cards having a newer number of the third and fourth sequence numbers to another card of the first and second cards (column 12, line 55-60).

As per claim 11, Claus teaches the ASM command is transmitted without setting the first sequence number to have the value of the second sequence number (column 8, lines 26-27).

As per claims 12 and 29, Claus teaches if the third sequence number corresponds to the fourth sequence number, performing a transaction between the first card and the second card (column 8, lines 22-23).

As per claims 13 and 51, Claus teaches the first key is a first global signing key, and the second key is a second global signing key, and wherein the first global signing key relates to the first sequence number, and the second global signing key relates to the second sequence number (column 12, lines 55-58).

As per claims 14 and 52, Claus teaches the first key is a first global signing key, and the second key is a second global signing key, and wherein the first global signing key is associated with a first value transfer protocol ("VTP") key, and the second global signing key is associated with a second VTP key, the first VTP key being stored in the

first storage device, the second VTP key being stored in the second storage device (column 4, line 67).

As per claims 15 and 53, Claus teaches each of the first portable device and the second portable device includes a processing device (column 4, line 67).

As per claim 16, Claus teaches receiving an authenticated system message which includes a command; and executing the command (column 8, lines 50-56).

As per claim 17, Claus teaches providing an application to at least one card of the first and second cards, the application is provided for at least one of: renewing a security feature of the at least one card, and updating a security scheme of the at least one card on-chip risk (column 7, line 54—column 8, line 7).

As per claim 18, Claus teaches providing a reference point for time to at least one of the first and second portable devices from a central command arrangement (column 7, line 62).

As per claim 19, Claus teaches enabling a selective targeting of at least one device of the first and second portable devices (column 8, lines 7-8); and applying re-customization procedures on the at least one device (column 7, lines 59-65).

As per claim 20, Claus teaches selecting a particular response by the at least one device when a predetermined criteria is met (column 8, lines 7-8).

As per claims 21 and 42, Claus teaches the first key is a first global signing key, and the second key is a second global signing key, and wherein the verification is performed by comparing cryptograms which are related to the first global signing key and the second global key (column 11, lines 13-16 and 24-25).

As per claim 22, Claus teaches generating the cryptograms by one of the first portable device and the second portable device (column 11, lines 24-25); and verifying the cryptograms using another one of the first portable device and the second portable device (column 11, lines 26).

As per claim 23, Claus teaches the cryptograms are generated by a central authority (column 2, lines 64-66).

As per claims 24, Claus teaches after the setting step, modifying stored parameters of at least one of the first and second cards to at least one of suspend, permit, and modify subsequent operations between the first and second cards or other cards (column 14, lines 53-60).

As per claims 30 and 57, Claus teaches the portable device is a smart card, and wherein the further portable device is a further smart card (column 2, line 44-46).

As per claim 33, Claus teaches if the second time is older than the first time, setting the second sequence number to have a value of the first sequence number (column 7, lines 63-65).

As per claims 34 and 38, Claus teaches after the setting step and if the first time is not equal to the second time, executing an action which is triggered by at least one of the first sequence number and the second sequence number (column 12, lines 44-47).

As per claim 35, Claus teaches after the executing step and. if the first time is not equal to the second time, performing a transaction between the first card and the second card (column 12, lines 49-50).

As per claims 36 and 49, Claus teaches if the first time is equal to the second time, performing a transaction between the first card and the second card (column 12, lines 49-50).

As per claim 39, Claus teaches wherein the portable device is a smart card, and the further portable device is a further smart card (column 2, lines 44-46), and wherein, after the execution of the particular action and if the first time is not equal to the second

time, the processing device performs a transaction between the smart card and the further smart card (column 12, lines 49-50).

As per claim 42, Claus teaches wherein the first key is a first global signing key, and the second key is a second global signing key, and wherein the verification is performed by comparing at least one first portion of the first global signing key to at least one second portion of the second global signing key (column 11, lines 13-16).

As per claim 44, Claus teaches wherein the verification succeeds when the at least one first portion corresponds to the at least one second portion (column 12, line 44).

As per claim 46, Claus teaches after the setting step, performing a transaction between the first card and the second card (column 12, lines 55-56).

As per claim 47, Claus teaches if the verification fails, suspending a transaction between the first card and the second card (column 11, line 18).

Claim Rejections - 35 USC ' 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 4 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Claus in view of Carlisle et al (USP 5,649,118).

As per claims 4 and 45, Claus teaches the method of encryption to secure the communication between two smart cards (column 3, lines 20-30). Claus fails to teach that the first and second global signing keys includes a private key and a public key, and wherein the verification is performed using the respective public keys. Carlisle et al teach the use of public and private keys to secure the communication using smart cards (column 8, lines 31-45). Private key cryptography is well known in the art. Private key

cryptography provides a very high level of security and is implemented in many applications.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Carlisle et al within the system of Claus because private key encryption is well established in the art and can be implemented using smart cards as taught by Carlisle et al.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

MV
Michael R Vaughan
Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100